4/30/2020

Zelealem, Tensaiye A

Manchester University

Blockchain Technology

Senior Project

Contents

[1. Introduction 2](#_Toc39142493)

[1.1. Audience 2](#_Toc39142494)

[1.2. Definitions 2](#_Toc39142495)

[2. What is Blockchain 3](#_Toc39142496)

[3. Characteristics of Blockchain Architecture 4](#_Toc39142497)

[4. General Blockchain Framework 5](#_Toc39142498)

[4.1. Transaction 5](#_Toc39142499)

[4.2. Wallet 5](#_Toc39142500)

[4.3. Signature 6](#_Toc39142501)

[4.4. Memory pool 6](#_Toc39142502)

[4.5. Network 6](#_Toc39142503)

[4.6. Consensus 6](#_Toc39142504)

[4.6.1. Proof of Work 7](#_Toc39142505)

[4.6.2. Proof of Stake 8](#_Toc39142506)

[4.7. Hashing 8](#_Toc39142507)

[4.8. Block 9](#_Toc39142508)

[4.9. Blockchain 9](#_Toc39142509)

[5. Bitcoin 9](#_Toc39142510)

[6. Ethereum 11](#_Toc39142511)

[6.1. EVM 12](#_Toc39142512)

[6.2. Smart Contract 12](#_Toc39142513)

[6.3. Solidity 12](#_Toc39142514)

[7. Decentralized Applications (dApps) 13](#_Toc39142515)

[8. Applications of Blockchain 14](#_Toc39142516)

[9. Voting System 15](#_Toc39142517)

[9.1. Why this project? 15](#_Toc39142518)

[9.2. Tools for Voting System 16](#_Toc39142519)

[9.2.1. Development Environment 16](#_Toc39142520)

[9.2.2. Metamask 16](#_Toc39142521)

[9.2.3. Ganache 16](#_Toc39142522)

[9.2.4. Front-end 17](#_Toc39142523)

[9.3. How it works? 18](#_Toc39142524)

[9.4. Improvements 19](#_Toc39142525)

[9.5. Benefits of Voting dApps 20](#_Toc39142526)

[10. Conclusion 20](#_Toc39142527)

[11. Resources 21](#_Toc39142528)

# Introduction

The following document is a research paper that provides an overview of the blockchain technology. The document discusses the purpose of blockchain, its framework, and its various applications. The document will also have an in-depth discussion about the first blockchain as well as the Ethereum blockchain since both are vital when discussing blockchain technology. Blockchain is a revolutionary technology that will impact the world immensely.

## Audience

This document is intended for the Mathematics and Computer Science department at Manchester University. It is also intended for juniors and seniors who are interested in a detailed overview of the blockchain technology. Readers knowledgeable with the blockchain technology are also welcomed to read this document.

## Definitions

|  |  |
| --- | --- |
| Blockchain | A digital ledger that holds records of transactional data. |
| Blocks | Containers that hold a bundle of transactional data. |
| Transactions | Data structures that encode a transfer of value from an input to an output |
| Smart Contract | A contract written in code. |
| EVM | Ethereum’s virtual machine responsible for executing smart contracts. |
| Turing Complete | A machine that performs the functionality of a Turing machine. |
| Solidity | Object-Oriented programming language used to write smart contracts. |
| Dapp | An application that runs on a distributed system. |
| Hash Value | A digital Fingerprint. |
| Gas Fee | The cost necessary to perform a transaction on the network. |
| Ether | The cryptocurrency of the Ethereum blockchain network. 1 Ether is currently worth approximately $210. |

# What is Blockchain?

A blockchain is a digital database that holds a record of transactional data. The data can be accessed by anyone with an internet connection. Blockchain is distributed meaning it stores information across a network of personal computers. Since it is both decentralized and distributed the system cannot be owned by one individual or an entity. Everyone can use and help run the system. This increases the system's security because it is difficult for anyone person to take down the network or corrupt it.

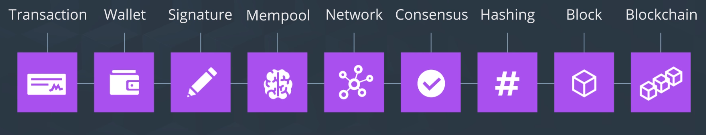
Each individual that accesses the system uses their computer to hold records submitted by others called blocks. These blocks use a method of math called cryptography to ensure the records cannot be changed or corrupted by anybody.

# Characteristics of Blockchain Architecture

* Cryptography: Blockchain transactions are very difficult to corrupt. Since every node has a copy of the ledger, to add a transaction each node in the blockchain must agree to the validity. All the blocks in the ledger come with a unique hash and the hash of the previous block. Thus, changing the data means changing the hash of all blocks, which is highly difficult.
* Immutability: All records made in blockchain cannot be changed or removed. Once a member has agreed on a transaction and it has been recorded it can never be changed. One can record a transaction to change the asset’s state, but one cannot hide the original transaction. “This gives the idea of provenance of assets, which means that for any asset you can tell where it is, where it’s been and what has happened throughout its life.” (Pattison 2017)
* Decentralization: The network does not have any single person or framework as the governing authority. The system is distributed; every member of the blockchain structure can directly access the system.
* Consensus: This is an algorithm blockchain uses to achieve reliability in the data. The algorithm requires agreement between the majorities to validate every new block. There are different types of consensus algorithms for different blockchain but essentially, they all have the same core concept.

# General Blockchain Framework

Understanding the blockchain framework allows us to understand how the blockchain works more clearly.



Fundamental Blockchain Frameworks

## Transaction

Transactions are made of multiple inputs and outputs. It is a data structure that encodes a transfer of value from an input to an output. Inputs in a transaction can be seen as unspent outputs from a different transaction.

## Wallet

A Wallet is used to establish one’s identity on the blockchain. A wallet is made up of three things a wallet address, a private key, and a public key. A wallet address is a unique identifier of one’s wallet. A private key consists of a secret number that allows the owner to spend bitcoin from their wallet. A public key is a sharable key that is given to others when a person wants other people to send them money.

## Signature

A signature is used to place proof of ownership for each transaction on the network. Signatures help prevent fraud. Signatures ensure the owner is the one that is sending the money.

## Memory pool

The memory pool, also known as the mempool, is a waiting place for all the transactions that have not been confirmed before they are added on to the blockchain. Since there are so many things happening, transactions have to wait in line before they can be validated.

## Network

The blockchain is supported by a distributed peer to peer network. A peer-to-peer network is a network of computers that permits information to be shared across users. This is done without the need for a central authority holding that information. The blockchain is not only a peer-to-peer network it is also a distributed network. This means the network is spread out across multiple nodes. Everyone downloads a copy of the blockchain to their local computer which allows them to interact with their copy of the blockchain and have full access to the information the blockchain contains.

## Consensus

Currently, there are many consensus algorithms but in the following two subsections, we will be discussing the Proof of Work and the Proof of Stake algorithms.

### Proof of Work

The proof of work algorithm is an algorithm the top cryptocurrencies (Bitcoin and Ethereum) currently use. This algorithm is one of many algorithms that can help reach consensus in a blockchain. One of the biggest questions in consensus is known as the Byzantine Generals’ problem. The following is the Byzantine Generals’ problem:

Imagine the byzantine empire has encircled a city, it has multiple battalions placed around the city, each battalion camped several miles apart and each led by a general. The generals and their lieutenants communicate with one another through messengers. A coordinated attack from all generals at the same time will be a success if there is high resistance, a coordinated retreat from all generals is also a success. An uncoordinated attack will result in defeat. If the generals, the lieutenants, and the messengers were all trustworthy there would be no issue and will result in a simple solution. But the problem is some of the messengers and a few generals are traitors. (Vaidya 2018)

How can one make sure that multiple generals separated by distance are in accord before an action has happened? The Byzantine Generals’ Problem is an analogy for the blockchain network. Instead of war, we are looking at the blockchain network and instead of generals think of nodes. In a distributed system one needs a way to guarantee trust between multiple parties when there is no form of communication.

Bitcoin solved this problem using the proof of work algorithm. The proof of work is an algorithm that can help reach consensus on the blockchain network. The node contains a copy of a computer program running the ledger. This ledger using cryptography records transactions and events in the exact order they happen. The ledgers displayed on every node are the same for everyone. As soon as a change is made to the ledger after it has been validated using a complex mathematical puzzle all copies of the ledger are simultaneous updated. This gives us a distributed ledger that is also in consensus. Thus, the problem is solved.

### Proof of Stake

The purpose of the proof of stake algorithm is like that of the proof of work algorithm. But they differ in the method they use to add blocks. In proof of work, miners solve a mathematical puzzle. “In POS, instead of miners, there are validators. The validators lock up some of their Ether as a stake in the ecosystem. Following that, the validators bet on the blocks that they feel will be added next to the chain. When the block gets added, the validators get a block reward in proportion to their stake.” (Rosic & Blockgeeks 2019). The difference between the two is that proof of stake focuses on giving votes to members, depending on how much stake they have in the success of the chain.

## Hashing

A Hash is a digital fingerprint for information. It is a unique string of letters and numbers that represents a set of data. In order to get a hashing value, one first starts with a set of data and passes it through a hashing function. The hashing function maps a group of data to a unique hash value. The hash value acts as a unique identifier for the original data. By referencing its hash value, one will be able to easily identify a given set of data.

## Block

A block is a container that holds a group of transactions to be added to the blockchain. As transactions are made, they are bundled together into blocks and added to the blockchain. This allows the ledger to be broken down into pieces to be managed more efficiently.

## Blockchain

A digital ledger that contains the history of all the transactions made on the network. All information on the blockchain is permanent and cannot be changed. In other words, the data is immutable. In order to construct a blockchain, both a hash value and a block are necessary. The hash values chain the blocks together in order from the recent block made to the genesis block (the first block ever created).

# Bitcoin

In 2008, a person or group of people that go by the name Satoshi Nakamoto published the Bitcoin whitepaper. In this document, Satoshi Nakamoto states there is a way to solve the vulnerabilities of traditional electronic payments involving third parties. The following are some of the vulnerabilities of the financial institutions that are stated in the Bitcoin Whitepaper:

* Transactions can be reversed
* Bank’s involvement results in an increase in transaction costs
* The system believes “A certain percentage of fraud is accepted as unavoidable.” (Satoshi)
* The possibility of transaction reversals requires people to trust a third party.

To solve the above flaws in the financial system, Satoshi proposed a peer-to-peer electronic cash system. By using cryptographic proof, there would be no need to trust the other party. This will enable two parties to transact directly without the need for a third party. Satoshi also states in the Whitepaper “Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers”. (Satoshi)

Although Satoshi was able to solve the problem caused by traditional financial institutions, there were some problems that occur only for digital currency. One problem that can exist in cryptocurrency is double-spending also known as the double-spend problem. Double-spending is the act of using the same electronic cash or in the case of Bitcoin a bitcoin token, more than once. In the case of physical money (cash), this does not occur because there is only one copy of the object. The double-spend problem was a problem developers and cryptographers were unable to solve since the early 1990s. (Asolo 2018) It was not until Satoshi Nakamoto’s Bitcoin that this problem was finally solved. Satoshi Nakamoto proposed a solution by using a timestamp server. According to Satoshi “A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post”. (Satoshi) Each timestamp contains the hash timestamp of the previous block creating a chain. To implement this on a peer-to-peer basis, Satoshi decided to use the proof of work system.

In 2009, Satoshi released the genesis block for Bitcoin. Bitcoin is the first-ever blockchain that is used to facilitate a financial transaction. “It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin blockchain network without the need for intermediaries.” (Rosic & Blockgeeks 2019)

In the following years, Bitcoin has transformed the global economy. Bitcoin is the most popular by far of all cryptocurrencies and the one with the highest number of users. According to the Bitcoin Market Journal, there are approximately 25 million bitcoin users globally and it is growing rapidly (Lielacher, Lielacher, & Cass Business School 2020).

# Ethereum

In 2013, Vitalik Buterin created the first second-generation blockchain. Vitalik was the co-founder of Bitcoin Magazine and lead writer. He understood the inner working of bitcoin and had a fundamental knowledge of how blockchains work. He realized bitcoin and other first-generation blockchains are not using the concept of blockchain to its fullest potential.

While Bitcoin and other first-generation blockchains possessed only one functionality (mostly cryptocurrency), Vitalik wanted to create a generalized platform that enables other developers to develop on top of it. Thus, he created Ethereum, an open-source programmable blockchain. In a similar manner that Satoshi wanted to remove third parties in financial transactions, Vitalik wanted to remove intermediaries for entire applications.

## EVM

The EVM, also known as the Ethereum Virtual Machine, is a powerful virtual machine, responsible for executing smart contracts. The following are some of the functionalities of the EVM:

* Process Turing-complete logic
* Confirms the correct amount of Ether value and validates the signature
* Calculates the transaction fee required and initializes the gas payment. (Katalyse.io 2018)

The gas payment is a cost that exists on the Ethereum platform. “It is the cost necessary to perform a transaction on the network.” (Frankenfield 2020) The more computational power an operation requires, the higher the gas cost will be. (Frankenfield 2020)

## Smart Contract

A smart contract is a digital contract and written in code. Smart contracts were first introduced by Ethereum, they enable developers to store data, to make decisions, interact with other smart contracts, and send Ether. They are also the fundamental piece of code that connects the front-end you have built to the Ethereum network. Ethereum allows software developers to code their own smart contracts. After they are built smart contracts have no owners, they belong to no one, and once created there is no way to take down a contract unless a kill switch has been implemented previously.

## Solidity

To be able to write smart contracts, one will need to use Solidity. Solidity is a high-level programming language created by Ethereum for the sole purpose of writing smart contracts. Python, JavaScript, and C++ were very influential to create this language and most developers say the language is very similar to them. According to Solidity’s documentation page “Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features”. (Solidity)

# Decentralized Applications (dApps)

Decentralized Applications are digital programs that have a backend code running on a decentralized peer-to-peer network. These programs are outside the scope of influence and control of a single authority. Standard application, like Facebook or Instagram, run on a centralized server. This means it is owned by an organization, and the entire application is controlled and influenced by that single authority. DApps run on blockchain networks in a decentralized environment and have no intervention or influence from a single authority. (Frankenfield 2020)

Since the EVM can run Turing complete logic, dApps can work in the same manner as standard applications. The only difference being the distributed network supports them.

There are multiple platforms like Ethereum that allows one to build decentralized applications. Once a backend is built that connects to the blockchain platform, one can build the front-end application the same way developers do for centralized applications.

# Applications of Blockchain

From the financial industry to the business industry, blockchain has the potential to change many industries all over the world. According to Business Insider Intelligence (2020), the following are a few industries blockchain can impact:

* Financial Industry
* Money Laundering Protection: Since blockchain enables record keeping, it supports the process in which a business can identify and verify the business’s clients.
* Insurance: Claims can be recorded on the blockchain. The blockchain will reject numerous claims on the same accident. This would help eliminate invalid claims.
* Government
* Identity Management: Utilizing the power of blockchain in identity management, establishing, identifying, and tracking identities is more efficient and secure. By providing only the minimum available information such as date of birth, individuals will be able to prove their identities.
* Voting: Blockchain technology has the potential to change the way people vote. It can make voting more accessible to people and more secure. In the next section, we will discuss how blockchain will be able to make voting more efficient as well as more effective.
* Business Industry
* Supply Chain Management: Due to the immutable nature of the blockchain, it can track a product throughout the supply chain life cycle. Sharing information on products through multiple companies as well as real-time tracking of these products can be difficult, but with the help of blockchain, it will be significantly more efficient. It will lead to more secure and clear monitoring of products. This will lead to a drastic reduction in time delay and human errors.
* Healthcare: Interoperability (Sharing health information) is currently one of the biggest problems in healthcare. Having health data saved on the blockchain can help deal with this problem. “As specialized connected medical devices become more common and increasingly linked to a person's health record, blockchain can connect those devices with that record. Devices will be able to store the data generated on a healthcare blockchain and append it to personal medical records.” (Business Insider Intelligence 2020)

The above are only a few instances in which blockchain can change the industries around the world.

# Voting System

I am building a decentralized application on the Ethereum blockchain that enables secure online voting for any private or public election. I have built a client-side web app that allows different users to cast votes for their desired candidate. This client-side application will communicate with an Ethereum smart contract that is connected to a local Ethereum Blockchain to deliver a secure voting experience.

## Why this project?

My senior research project was motivated by the corruption that has been evident during Ethiopia’s elections over the last decade. Having witnessed elections in which the government in power won 99% and 100% of the votes, I was motivated to work with blockchain technologies to develop systems that allow countries like Ethiopia to have both a fair and free election. I want to use blockchain technology since I believe it has the power to fundamentally change the future of voting and make it more accessible and secure.

## Tools for Voting System

There are a few tools necessary to build the Decentralized Voting System. The next subsections will discuss the purpose of the tools as well as the development environment needed to build and run the system. Multiple platforms allow developers to build decentralized applications, but I decided on using Ethereum since it is the world’s leading platform for building decentralized applications.

### Development Environment

I decided to use Node.js as the primary high-level coding language to build the voting system because I found it easier to integrate the multiple tools necessary for blockchain development in the Node ecosystem.

### Metamask

Metamask is a chrome extension that brings Ethereum to your browser. To interact with a decentralized app, I needed to get access to the Ethereum blockchain. Using Metamask enables me to set up accounts that will interact directly with Ethereum. “MetaMask manages your Ethereum wallet, which contains your Ethers (or money), and allows you to send and receive Ethers through a dApp of interest.” (Choi 2018)

### Ganache

We will need to create a private Ethereum blockchain that enables us to run tests and execute commands. Managing accounts and ether (test ether) can be difficult and take a lot of time. For this, we will be using Ganache. Ganache allows me to create a private Ethereum blockchain without any costs. It enables me to deploy contracts to develop applications for test purposes and it will manage accounts and ether for test purposes.

### Front-end

I have created a website for the users to be able to vote for the candidate of their desire. The website displays a list of candidates for the election. From the list users can choose their desired candidate, once they have chosen, Metamask will connect them to the Ethereum blockchain and ask them to verify the gas fee and make sure that they want to make the transaction. After the user verifies the transaction the desired candidate vote count is incremented and the transaction gas fee is deducted from the users' account. The website will then refresh and show the desired candidate received a vote.

## How it works?

A close up of a map

Description automatically generated

Diagram 1.0: Secure Voting System Architecture

The above diagram is a high-level diagram that better illustrates the Secure Voting Systems Architecture. Ganache allows us to set up a personal blockchain to test our Smart Contract. Ganache also provides us with 10 accounts preloaded with 100 Ethers each (for testing purposes). Metamask allows us to connect our browser to our local Ethereum blockchain provided by Ganache. We will not be able to connect to the main Ethereum network because that will cost actual Ether. Using Metamask we will also import one of the accounts Ganache provides. Now we have an account on Metamask with 100 test Ethers, so we can pay for our transactions. Before we run our dApp we need to compile our smart contract. Once that is done, we run our dApp which takes us to our website. The website provides a list of candidates to vote for. Once the voter has selected their desired candidate and clicks the vote button, Metamask will pop up, show you the necessary transaction fee (gas fee) and will ask you to verify the transaction. Once that goes through, the voter has made a confirmed transaction on the network, the site will reload and increase the desired candidates vote count. The site then removes the option of making another vote, to prevent a voter from voting more than once.

## Improvements

The Secure Voting System was just a prototype so, it has plenty of room for improvements. One of the major problems I am currently facing is finding a way to prevent people who have multiple accounts on Metamask from being able to get multiple votes in. One solution to this problem is to require voters to scan their driver’s license or passport and have biometrics (Fingerprint or Iris scan) before they vote. The biometrics will help verify if the person who has submitted the driver’s license or the passport is the same as the person who is voting. But by implementing the above solution it leads to another problem, maintaining anonymity. To prevent people from influencing other people’s votes, we should be able to maintain anonymity. The information voters provide in order to verify their votes needs to be hidden. According to Garner, “There are different ways to accomplish this, including zero knowledge proofs, ring transactions, or various encryption methods. Each has its benefits, drawbacks, and technical challenges.” Although there are ways to try and hide the voter’s information, Garner states “True anonymity at the same time as verified identity is the big challenge of blockchain voting.” (Bennet Garner 2019)

## Benefits of Voting DApps

Integrating blockchain technology into Voting Systems has various benefits. According to Bennet Garner (2019), the following are some of the important benefits the Voting DApps can provide:

* Transparency: Once the voter has made their vote, they will be able to track it through the blockchain forever.
* Security: The security of the DApp is as secure as the blockchain. With a good consensus algorithm and a large network size, cybersecurity experts believe it is invulnerable.
* Real-Time Voting: Due to its transparency, it allows voters to follow the vote count in real-time. Also, since there is no need for counting ballots it happens at a much shorter period.
* Increased Voter Engagement: If through blockchain digital voting is viable, voting will be drastically simplified. Anyone with a computer or a smartphone will easily be able to vote within minutes. This will allow for a significant increase in voter turnouts.

The above are only some of the advantages of having a blockchain voting system. Other advantages include anonymity (to a certain extent), shortened processing time, and decentralization (no company or even the government will have ownership of the system).

# Conclusion

Blockchain technology has the potential to change many industries all over the world. Blockchain platforms like Ethereum have allowed developers to create decentralized applications, which enabled us to create leaderless (controlled by the users), secure, and more stable applications. My Secure Voting project allowed me to understand how to build a decentralized application. Apart from the smart contract and the backend necessary to connect to the Ethereum blockchain, building a DApp is very similar to building a centralized application. This means any developer with minimal training can easily develop DApps.

Blockchain will transform leading industries such as healthcare, finance, business, and banking. It offers security, transparency, anonymity, and accountability.

The blockchain system is decentralized and distributed no one person owns it, but everyone in the network has access to it and can help run it. From the customer’s point of view, this represents a transparent system and they will be a part of a more inclusive system.

For this project, I have successfully been able to understand the inner workings of blockchain technology and create a decentralized application. The benefits of blockchain are so immense I believe it is safe to say it is as revolutionary as the internet.

# Resources

Asolo, Bisade. “Double-Spending Explained.” *Mycryptopedia*, 21 Dec. 2018, [www.mycryptopedia.com/double-spending-explained/](http://www.mycryptopedia.com/double-spending-explained/).

Choi, Sean. “What Is MetaMask? Really... What Is It?” *Medium*, Medium, 11 Sept. 2018, [medium.com/@seanschoi/what-is-metamask-really-what-is-it-7bc1bf48c75](mailto:medium.com/@seanschoi/what-is-metamask-really-what-is-it-7bc1bf48c75).

Frankenfield, Jake. “Gas (Ethereum).” *Investopedia*, Investopedia, 29 Jan. 2020, [www.investopedia.com/terms/g/gas-ethereum.asp](http://www.investopedia.com/terms/g/gas-ethereum.asp).

Frankenfield, Jake. “Decentralized Applications – DApps.” *Investopedia*, Investopedia, 29 Jan. 2020, [www.investopedia.com/terms/d/decentralized-applications-dapps.asp](http://www.investopedia.com/terms/d/decentralized-applications-dapps.asp).

Garner, Bennet. “How Blockchain Voting Works & Why We Need It.” *CoinCentral*, 14 May 2019, coincentral.com/how-blockchain-voting-works-why-we-need-it/.

Intelligence, Business Insider. “The Growing List of Applications and Use Cases of Blockchain Technology in Business and Life.” *Business Insider*, Business Insider, 2 Mar. 2020, [www.businessinsider.com/blockchain-technology-applications-use-cases](http://www.businessinsider.com/blockchain-technology-applications-use-cases).

Katalyse.io. “Blockchain Basics - What Is EVM.” *Medium*, CryptoDigest, 6 July 2018, cryptodigestnews.com/blockchain-basics-what-is-evm-52d83616764.

Lielacher, Alex, et al. “How Many People Use Bitcoin in 2020?” *Bitcoin Market Journal*, 11 Feb. 2020, [www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/](http://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/).

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 2008.

Pattison, Ian. “4 Characteristics That Set Blockchain Apart.” *Cloud Computing News*, 7 Apr. 2017, [www.ibm.com/blogs/cloud-computing/2017/04/11/characteristics-blockchain/](http://www.ibm.com/blogs/cloud-computing/2017/04/11/characteristics-blockchain/).

Rosic, Ameer, and Blockgeeks. “What Is Bitcoin? [The Most Comprehensive Step-by-Step Guide] Updated!” *Blockgeeks*, 13 Aug. 2019, blockgeeks.com/guides/what-is-bitcoin/.

Rosic, Ameer, and Blockgeeks. “Proof of Work vs Proof of Stake: Basic Mining Guide.” *Blockgeeks*, 23 Aug. 2019, blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.

“Solidity.” *Solidity*,solidity.readthedocs.io/en/v0.6.4/#.

Thompson, Emma, et al. “The Benefits of Blockchain Voting.” *Coin Rivet*, 24 June 2019, coinrivet.com/the-benefits-of-blockchain-voting/.

Vaidya, Kiran. “The Byzantine Generals' Problem.” *Medium*, All Things Ledger, 1 June 2018, medium.com/all-things-ledger/the-byzantine-generals-problem-168553f31480.